## CLAIMS

1. A method of monitoring operation of a processing system (A, B,..., X) including system resources and having a plurality of processes running thereon, characterized in that it includes the step of monitoring, for at least two processes in said plurality, a set of system primitives that allocate or release said system resources.

2. The method of claim 1, characterized in that said set of primitives monitored includes all the system primitives that allocate or release said system resources.

3. The method of claim 1, characterized in that said set of primitives monitored includes exclusively those system primitives that allocate or release said system resources.

4. The method of claim 1, characterized in that monitoring said system primitives includes at least one of:

- tracking (105a, 105b) the processes running on said system and monitoring resources used thereby,
- monitoring (105c) connections by said processes running on said system,
- monitoring (105d) the file-related operations performed within said system, and
- monitoring (105a) operation of commonly used modules with said system.

5. The method of claim 1, wherein said set of primitives monitored identifies a state of said processing system, the method further including the steps of:

- recording (104) a current state of said system over a current period of time and a previous state of the system over a previous period of time,

- revealing any differences between said current state of the system and said previous state of the system, and

- detecting any such difference revealed as a likely anomaly in the system.

6. The method of claim 5, characterized in that said anomaly detection includes a learning stage (601) to generate said previous state of the system based on said learning stage (601).

7. The method of claim 5, characterized in that said anomaly detection includes the step of correlating a plurality of said anomalies detected (106) and decide whether these identify a dangerous event for the system.

8. The method of claim 7, characterized in that it includes the step of emitting an alert signal (106, 107) indicative of any dangerous event for the system identified.

9. The method of claim 7, characterized in that it includes the steps of:

- generating a sequence of said anomalies (106),

- producing a sequence of pre-conditions in a rule base, and

- if said sequence of anomalies at least loosely matches said sequence of pre-conditions, issuing a resulting alert signal.

10. The method of claim 7, characterized in that it includes the step of assigning respective weights to said anomalies in said plurality, each said weight being indicative of the criticality of the event represented by the anomaly to which the weight is assigned.

11. The method of claim 8, characterized in that said step of correlating includes associating with each anomaly a value of the weight at the previous alert

signal emission time plus the current value modulated with an exponential decay factor, whereby the significance thereof decreases over time.

12. The method of claim 11, characterized in that said processing system operates on process identifiers (PID), whereby a plurality of anomalies are detected for the same process identifier and said anomalies are aggregated over time according the following formula:

$$W_{i+1}(t) = W_i(T_{i+1} - T_i) + LA_{i+1} \cdot \exp\left(-\frac{t - T_i}{\tau}\right)$$

$$W_0 = 0$$

where $W_i$ is the weight of a user level alert signal associated to the common stream of anomalies, when the i-th anomaly is detected; $T_i$ is the time of detection of the i-th anomaly, $LA_i$ is the weight associated to the i-th anomaly and $\tau$ is a time-decay constant.

13. The method of claim 7, characterized in that said step of correlating includes the step of mapping said anomalies in said plurality into respective fuzzy sets.

14. The method of claim 5, characterized in that said monitoring includes intercepting (110) low-level data within said system watching for changes in the state of the system thus providing data to be analyzed in said anomaly detection.

15. The method of claim 1, characterized in that it includes the step of providing a plurality of modules for performing said monitoring, said plurality of modules being comprised of a first set of components (101, 102, 103) depending on the system being monitored and the second set of components (104, 105, 106) that are independent of the system being monitored.

16. The method of claim 15, characterized in that it includes the step of providing within said first set of modules at least one module selected out of the group consisting of:

- a device driver (101), for intercepting the system calls associated with said primitives in said set,
- a kernel information module (102) configured for reading information for all processes running on said monitored system, and
- a system call processor (103) configured for reading the binary data related to the system calls of said system and translating them into respective higher-level system call abstractions.

17. The method of claim 5, characterized in that it includes the step of monitoring all processes running on the system monitored and all file descriptors and the socket description used by each said process to produce an instantaneous state of the system monitored.

18. Apparatus for monitoring operation of a processing system (A, B, ..., X) including system resources and having a plurality of processes running thereon, characterized in that it includes analysis modules (105) configured for monitoring, for at least two processes in said plurality, a set of system primitives that allocate or release said system resources.

19. The apparatus of claim 18, characterized in that said analysis modules (105) are configured for monitoring all the system primitives that allocate or release said system resources.

20. The apparatus of claim 18, characterized in that said analysis modules (105) are configured for monitoring exclusively those system primitives that allocate or release said system resources.

21. The apparatus of claim 18, characterized in that said analysis modules (105) are selected out of the group consisting of:

- at least one application knowledge module (105a, 105b) tracking the processes running on said system and monitoring resources used thereby,
- a network knowledge module (105c) monitoring connections by said processes running on said system,
- a file-system analysis module (105d) monitoring the file-related operations performed within said system, and
- a device monitoring module (105a) monitoring operation of commonly used modules with said system.

22. The apparatus of claim 18, characterized in that, wherein said set of primitives monitored identifies a state of said processing system, the apparatus includes a detection component (120; 104, 105, 106) configured for recording (104) a current state of said system over a current period of time and a previous state of the system over a previous period of time, revealing any differences between said current state of the system and said previous state of the system, and detecting any such difference revealed as a likely anomaly in the system.

23. The apparatus of claim 22, characterized in that said detection component (120; 104, 105, 106) is configured for running a learning stage (601) to generate said previous state of the system based on said learning stage (601).

24. The apparatus of claim 22, characterized in that said detection component (120; 104, 105, 106) is configured for correlating a plurality of said anomalies detected (106) and decide whether these identify a dangerous event for the system.

25. The apparatus of claim 24, characterized in that said detection component (120; 104, 105, 106) is configured for emitting an alert signal (106, 107) indicative of any dangerous event for the system identified.

26. The apparatus of claim 24, characterized in that said detection component (120; 104, 105, 106) is configured for:

- generating a sequence of said anomalies (106),
- producing a sequence of pre-conditions in a rule base, and
- if said sequence of anomalies at least loosely matches said sequence of pre-conditions, issuing a resulting alert signal.

27. The apparatus of claim 24, characterized in that said detection component (120; 104, 105, 106) is configured for assigning respective weights to said anomalies in said plurality, each said weight being indicative of the criticality of the event represented by the anomaly to which the weight is assigned.

28. The apparatus of claim 25, characterized in that said detection component (120; 104, 105, 106) is configured for associating with each anomaly a value of the weight at the previous alert signal emission time plus the current value modulated with an exponential decay factor, whereby the significance thereof decreases over time.

29. The apparatus of claim 28, characterized in that, said processing system operating on process identifiers (PID), whereby a plurality of anomalies are detected for the same process identifier, said detection component (120; 104, 105, 106) configured for aggregating said anomalies over time according the following formula:

$$W_{i+1}(t) = W_i(T_{i+1} - T_i) + LA_{i+1} \cdot \exp\left(-\frac{t - T_i}{\tau}\right)$$

$$W_0 = 0$$

where $W_i$ is the weight of a user level alert signal associated to the common stream of anomalies, when the i-th anomaly is detected; $T_i$ is the time of detection of the i-th anomaly, $LA_i$ is the weight associated to the i-th anomaly and $\tau$ is a time-decay constant.

30. The apparatus of claim 24, characterized in that said detection component (120; 104, 105, 106) is configured for correlating said anomalies in said plurality by mapping them into respective fuzzy sets.

31. The apparatus of claim 22, characterized in that said monitoring includes an information gathering component (110) configured for intercepting low-level data within said system watching for changes in the state of the system thus providing data to be analyzed in said anomaly detection.

32. The apparatus of claim 18, characterized in that it includes a plurality of modules for performing said monitoring, said plurality of modules being comprised of a first set of components (101, 102, 103) depending on the system being monitored and a second set of components (104, 105, 106) that are independent of the system being monitored.

33. The apparatus of claim 32, characterized in that said first set of modules includes at least one module selected out of the group consisting of:

- a device driver (101), for intercepting the system calls associated with said primitives in said set,
- a kernel information module (102) configured for reading information for all processes running on said monitored system, and

- a system call processor (103) configured for reading the binary data related to the system calls of said system and translating them into respective higher-level system call abstractions.

34. The apparatus of claim 22, characterized in that it includes a current state module (104) monitoring all processes running on the system monitored and all file descriptors and the socket description used by each said process to produce an instantaneous state of the system monitored.

35. A computer program product loadable in the memory of at least one computer and including software code portions for performing the steps of the method of any claims 1 to 17.